UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/698,507	10/26/2000	Rolf E. Carlson	xRCa-12	3367

20995 7590 12/11/2006

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

EXAMINER
HOFFMAN, BRANDON S

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 12/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/698,507	**Applicant(s)** CARLSON, ROLF E.	
	Examiner Brandon S. Hoffman	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _22 September 2006_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-70_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-70_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _11-14-06_.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-70 are pending in this office action.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on September 22, 2006, has been entered.

3. Applicant's arguments, filed March 6, 2006, are moot in view of the new ground of rejection.

Rejections

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

5. Claims 1-70 are rejected under 35 U.S.C. 103(a) as being unpatentable over Falciglia (U.S. Patent No. 5,971,849) in view of Ramasubramani et al. (U.S. Patent No. 6,233,577).

Regarding claims 1-70, Falciglia teaches a casino environment, wherein gaming servers are connected to gaming machines, and users are remotely connected, through the internet or other networking means, to play poker and other casino games (see fig. 2). Falciglia fails to disclose the security aspects and the gaming machines, except for the use of a password. However, Ramasubramani et al. teaches a client and server environment, with the security aspects, such as the public/private key encryption, timestamps, and certificates. The combination of Falciglia and Ramasubramani et al. thus arrives at the claimed invention, as described below.

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine security for gaming, such as a plurality of **private** keys and public keys, a random number generator that generates said plurality of **private** keys, an encryption algorithm, timestamps, and a certificate authority, as taught by Ramasubramani et al., with the gaming machines of Falciglia. It would have been obvious for such modifications because the security of Ramasubramani et al. provides piece of mind that the data transmitted from one gaming machine to another is secure and legit, so that the appeal of functionality of the online gambling flourishes.

Regarding claims 1, 11-13, 17, and 47, Falciglia as modified by Ramasubramani et al. teaches a casino gaming system, comprising:

- A plurality of gaming machines configured to determine an outcome of a game (fig. 2, ref. num 50/52 and col. 5, line 59 through col. 6, line 3 of Falciglia);

- A gaming server configured to determine an outcome of a game (fig. 2, ref. num 64 of Falciglia), said gaming server comprising:
    - A plurality of **private** keys (fig. 3, ref. num 326 of Ramasubramani et al.),
    - Each of said plurality of **private** keys including a time stamp, said time stamp indicating a period of time for which each of said plurality of **private** keys is used (col. 10, lines 47-59);
    - A random number generator that generates said plurality of **private** keys; and an encryption algorithm (col. 10, line 60 through col. 11, line 17 of Ramasubramani et al.),
- A network bus interconnecting said plurality of gaming machines and said gaming server, said network bus used to transmit information between said plurality of gaming machines and said gaming server (fig. 2, ref. num 56 of Falciglia),
- Said gaming server using said encryption algorithm to encrypt at least one of said plurality of **private** keys (col. 4, lines 29-50 of Ramasubramani et al.),
- Said gaming server transmitting said at least one of said plurality of **private** keys over said network bus to at least one of said plurality of gaming machines where said key is decrypted (col. 4, lines 29-50 of Ramasubramani et al.),
- Said at least one of said plurality of gaming machines using said at least one of said plurality of **private** keys to encrypt said information (fig. 1, step 5 of Ramasubramani et al., client encrypts the session key),

- Said at least one of said plurality of gaming machines transmitting said encrypted information over said network bus to **a** remote machine (fig. 1, step 5 of Ramasubramani et al., client sends the encrypted session key over the network).

Regarding claim 25, Falciglia as modified by Ramasubramani et al. teaches a method for communicating information using a casino gaming system having at least one gaming machine and a gaming server, said method comprising:

- Receiving a request on said gaming server from a remote machine to initiate game play on said at least one gaming machine (fig. 10, ref. num 158 of Falciglia);
- Establishing a first communication link between said at least one gaming machine and said gaming sever (fig. 2, ref. num 56 of Falciglia);
- First transmitting at least one of a plurality of **private** keys stored at said gaming server over said first communication link from said gaming server to said at least one gaming machine (col. 4,lines 29-50 of Ramasubramani et al.);
- Encrypting information sent from said at least one gaming machine using said at least one of said plurality **private** keys (fig. 1, step 5 of Ramasubramani et al., client encrypts session key);
- Determining an outcome of said game play on said at least one gaming machine (col. 5, line 59 through col. 6, line 3 of Falciglia);

- Second transmitting said encrypted information over said first communication link from said at least one gaming machine to said remote machine (fig. 1, step 5 of Ramasubramani et al., client sends the encrypted session key over the network);
- Receiving encrypted information from said remote machine; and decrypting said received encrypted information using said at least one of said plurality of **private** keys (col. 5, lines 27-47 of Ramasubramani et al.).

Regarding claim 38, Falciglia as modified by Ramasubramani et al. teaches a casino gaming system for communicating information using asymmetric key pairs that includes a private key and a public key, said casino gaming system comprising:

- A plurality of gaming machines, each configured to determine an outcome of a game of game play and provide said outcome to a remote machine (fig. 2, ref. num 50/52 and col. 5, line 59 through col. 6, line 3 of Falciglia);
- A certificate authority server including a memory storing at least a plurality of said public keys **and at least a plurality of private keys** of said asymmetric key pairs (fig. 3, ref. num 114 and 326 of Ramasubramani et al.);
- A network bus interconnecting said plurality of gaming machines and said certificate authority server (fig. 2, ref. num 56 of Falciglia),
- Said certificate authority server transmitting at least one of said plurality of public keys **and at least one of said plurality of private keys** over said network bus to at least one of said plurality of gaming machines wherein said certificate authority

server signs said at least one of said plurality of public keys transmitted over said network bus (col. 4, lines 29-50 of Ramasubramani et al.),

- Said at least one of said plurality of gaming machines using said at least one of said plurality of said **private** keys to encrypt information (fig. 1, step 5 of Ramasubramani et al., client encrypts session key),
- Said at least one of said plurality of gaming machines transmitting said encrypted information over said network bus to said remote machine (fig. 1, step 5 of Ramasubramani et al., client sends the encrypted session key over the network).

Regarding claims 49 and 55-57, Falciglia as modified by Ramasubramani et al. teaches a casino gaming system connected to at least one outside computer via an outside network, said casino gaming system comprising:

- A gaming server (fig. 2, ref. num 64 of Falciglia);
- A plurality of gaming machines located in a casino and configured to determine an outcome of a game (fig. 2, ref. num 50/52 and col. 5, line 59 through col. 6, line 3 of Falciglia),
- Wherein said gaming server is configured to receive a request to initiate game play on at least one of the gaming machines from said at least one outside computer (fig. 10, ref. num 158 of Falciglia), and
- Configured to provide at least one **private** encryption key to said at least one of the gaming machines, and wherein said at least one of the gaming machines is

configured to use said at least one encryption key to communicate with said at least one outside computer (col. 4, lines 29-50 of Ramasubramani et al.);

- A plurality of access switches, each one of said plurality of access switches individually connected to a different one of said plurality of gaming machines (col. 5, lines 48-58 of Falciglia); and
- A network bus connected to said gaming server and each of said plurality of access switches (fig. 2, ref. num 56 of Falciglia);
- Said outside network connected to said gaming server (fig. 2, ref. num 56 of Falciglia),
- One of said plurality of access switches connecting one of said plurality of gaming machines and said outside computer over said outside network when said one of said plurality of gaming machines is idle, so as to enable a remote player of said outside computer to play said one of said plurality of gaming machines, the other of said plurality of access switches disconnecting said outside computer from the other of said plurality of gaming machines (col. 5, lines 48-58 of Falciglia).

Regarding claims 58, 68, and 70, Falciglia as modified by Ramasubramani et al. teaches a method for communicating with a plurality of gaming machines in a casino, said plurality of gaming machines connected to a gaming server, said method comprising the steps of:

- Receiving on a gaming server a request from an outside network for an identified one of said plurality of gaming machines, said request initiated by a remote player (fig. 10, ref. num 158 of Falciglia);
- Providing **at least one private** encryption key to said identified one of said plurality of gaming machines (col. 4, lines 29-50 of Ramasubramani et al.);
- Determining the outcome of a game on said identified one of said plurality of gaming machines (col. 5, line 59 through col. 6, line 3 of Falciglia);
- Transmitting data encrypted using said encryption key from said identified one of said plurality of gaming machines over a secured communication link between said outside network and said identified one of said plurality of gaming machines when said identified one of said plurality of gaming machines is idle (col. 5, lines 48-58 of Falciglia),
- So as to enable the remote player to play a casino game at said identified one of said plurality of gaming machines (fig. 1, step 6 of Ramasubramani et al., a secure connection is created); and
- Delivering to said outside network a gaming machine unavailable message when said identified one of said plurality of gaming machines is in use (col. 5, lines 48-58 of Falciglia).

Regarding claims 2-5, 18, 19, 26, 27, and 54, the examiner takes Official notice that said plurality of **private** keys are symmetric session keys, wherein the keys use

DES or triple-DES algorithms. It would have been obvious to use symmetric session keys because symmetric keys are faster.

Regarding claims 6, 20, 28, and 53, Falciglia as modified by Ramasubramani et al. teaches wherein said plurality of **private** keys comprise asymmetric key pairs (see col. 3, line 60 through col. 4, line 8 of Ramasubramani et al.).

Regarding claims 7, 21, and 29, Falciglia as modified by Ramasubramani et al. teaches wherein said asymmetric keys are session keys (see col. 3, lines 48-59 of Ramasubramani et al.).

Regarding claim 8, Falciglia as modified by Ramasubramani et al. teaches wherein said asymmetric key pairs comprise Rivest, Shamir, and Adleman (RSA) algorithms (see col. 4, lines 3-8 of Ramasubramani et al.).

Regarding claims 9, 30, and 40, Falciglia as modified by Ramasubramani et al. as modified by Ramasubramani et al. teaches wherein said gaming server is interconnected to an outside network (see fig. 2, ref. num 56 of Falciglia).

Regarding claims 10, 31, 41, 50, and 67, Falciglia as modified by Ramasubramani et al. teaches wherein said outside network is the Internet (see fig. 2, ref. num 56 of Falciglia).

Regarding claims 14, 22, and 42, Falciglia as modified by Ramasubramani et al. teaches wherein said encrypted information is transmitted over said network bus to another of said at least one gaming machines (see fig. 2, ref. num 56 of Falciglia).

Regarding claims 15, 23, and 43, Falciglia as modified by Ramasubramani et al. teaches wherein said encrypted information is transmitted over said network bus to said gaming server (see fig. 2, ref. num 56 of Falciglia).

Regarding claims 16, 24, and 44, Falciglia as modified by Ramasubramani et al. teaches further comprising:

- An outside network connected to said gaming server (see fig. 2, ref. num 56 of Falciglia); and
- A remote machine connected to said outside network wherein said encrypted information is transmitted over said network bus and said outside network to said remote machine (see fig. 2, ref. num 50 of Falciglia).

Regarding claims 32 and 46, Falciglia as modified by Ramasubramani et al. teaches wherein said gaming server further comprises a random number generator that generates said plurality of **private** keys (see col. 10, line 60 through col. 11, line 17 of Ramasubramani et al.).

Regarding claim 33, Falciglia as modified by Ramasubramani et al. teaches further comprising the steps of encrypting each of said plurality of **private** keys transmitted from said gaming server to said at least one gaming machine (see col. 5, lines 41-47 of Ramasubramani et al.).

Regarding claim 34, Falciglia as modified by Ramasubramani et al. teaches wherein said step of second transmitting further comprises transmitting said encrypted information over said first communication link to another of said at least one gaming machine (see fig. 2, ref. num 52 of Falciglia), and wherein said step of decrypting further comprises decrypting said received encrypted information at said another of said at least one gaming machine (see fig. 2, ref. num 52 of Falciglia).

Regarding claim 35, Falciglia as modified by Ramasubramani et al. teaches wherein said step of transmitting further comprises second transmitting said encrypted information over said first communication link to said gaming server, and wherein said step of decrypting further comprises decrypting said received encrypted information at said gaming server (see fig. 2, ref. num 64 of Falciglia).

Regarding claim 36, Falciglia as modified by Ramasubramani et al. teaches further comprising the step of establishing a second communication link between said gaming server and a remote machine (see fig. 2, connection between 114 and 110 of Ramasubramani et al.).

Regarding claim 37, Falciglia as modified by Ramasubramani et al. teaches wherein said step of transmitting further comprises transmitting said encrypted information over said first communication link and said second communication link to said remote machine, and wherein said step of decrypting further comprises decrypting said received encrypted information at said remote machine (see col. 9, lines 8-47 of Ramasubramani et al.).

Regarding claim 39, Falciglia as modified by Ramasubramani et al. teaches wherein each of said plurality of gaming machines validates said at least one of said signed plurality of public keys received from said network bus (see col. 3, lines 57-59 of Ramasubramani et al.).

Regarding claim 45, Falciglia as modified by Ramasubramani et al. teaches wherein said network bus is connected to at least one gaming server, said certificate authority server transmitting at least one of said plurality of said public keys to said at least one gaming server, said gaming server encrypts information using said at least one of said plurality of said public keys, said gaming server transmits said encrypted information over said network bus (see col. 5, lines 41-47 of Ramasubramani et al.).

Regarding claim 48, Falciglia as modified by Ramasubramani et al. teaches wherein said network bus is connected to a plurality of other certificate authority servers (see fig. 4A, ref. num 356 and 358 of Ramasubramani et al.), said certificate authority server transmitting at least one of said plurality of said public keys to said plurality of other certificate authority servers wherein said plurality of other certificate authority servers encrypts information using said at least one of said plurality of said public keys and transmits said encrypted information over said network bus (see col. 4, lines 29-41 of Ramasubramani et al.).

Regarding claim 51, the combination of Falciglia in view of Ramasubramani et al. teaches further comprising a certificate authority server connected to said network bus, said certificate authority server including a plurality of public keys of a plurality of asymmetric key pairs (see fig. 3, ref. num 124 of Ramasubramani et al.).

Regarding claim 52, the combination of Falciglia in view of Ramasubramani et al. teaches wherein said outside computer acquires one of said plurality of public keys from said certificate authority server via said outside network and said network bus, said outside computer using said one of said plurality of public keys to encrypt information transmitted to said one of said plurality of gaming machines over said outside network and said network bus (see fig. 1, step 5 of Ramasubramani et al.).

Regarding claim 59, the combination of Falciglia in view of Ramasubramani et al. teaches wherein said step of receiving a request further comprising entering player identification information; and providing said entered player identification information to a database (see col. 7, lines 10-32 of Ramasubramani et al.).

Regarding claim 60, the combination of Falciglia in view of Ramasubramani et al. teaches wherein said step of providing said entered player identification information further comprises:

- Comparing said entered player identification information to said database (see col. 7, lines 10-32 of Ramasubramani et al.); and
- Providing said secured communication link between said outside network and said identified one of said plurality of gaming machines if said entered identification information matches an entry in said database (see col. 7, lines 10-32 of Ramasubramani et al.).

Regarding claim 61, the combination of Falciglia in view of Ramasubramani et al. teaches wherein said entered player identification information is credit card information (see col. 11, lines 11-23 of Falciglia).

Regarding claim 62, the combination of Falciglia in view of Ramasubramani et al. teaches further comprising the steps of documenting information about the remote player (see fig. 10, ref. num 152 of Falciglia).

Regarding claim 63, the combination of Falciglia in view of Ramasubramani et al. teaches wherein said documented information comprises information about the remote player (see col. 11, lines 11-23 of Falciglia).

Regarding claim 64, the combination of Falciglia in view of Ramasubramani et al. teaches wherein said documented information comprises a time for which the remote player plays said one of said plurality of gaming machines (see col. 11, lines 11-23 of Falciglia).

Regarding claim 65, the combination of Falciglia in view of Ramasubramani et al. teaches wherein said documented information comprises a location from which the remote player is playing (see col. 11, lines 11-23 of Falciglia).

Regarding claim 66, the combination of Falciglia in view of Ramasubramani et al. teaches wherein said documented information comprises an amount the remote player has wagered (see fig. 10, ref. num 186 of Falciglia).

Regarding claim 69, the combination of Falciglia in view of Ramasubramani et al. teaches wherein said plurality of gaming machines are located in a casino (see col. 5, lines 33-39 of Falciglia).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

BH

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

12/7/06